(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 977 452 A3

(12) **EUROPEAN PATENT APPLICATION**

(88) Date of publication A3:
20.12.2000 Bulletin 2000/51

(51) Int Cl.[7]: **H04Q 7/38**, H04L 9/08

(43) Date of publication A2:
02.02.2000 Bulletin 2000/05

(21) Application number: **99305705.8**

(22) Date of filing: **20.07.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **31.07.1998 US 127768**

(71) Applicant: **LUCENT TECHNOLOGIES INC.**
Murray Hill, New Jersey 07974-0636 (US)

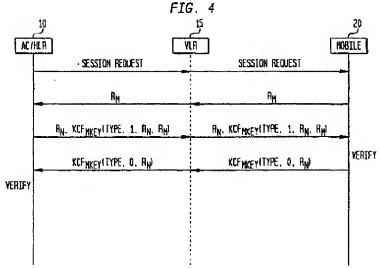
(72) Inventor: **Patel, Sarvar**
Montville, New Jersey 07045 (US)

(74) Representative:
Buckley, Christopher Simon Thirsk et al
Lucent Technologies (UK) Ltd,
5 Mornington Road
Woodford Green, Essex IG8 0TU (GB)

(54) **Method for updating secret shared data in a wireless communication system**

(57) In the method for updating secret shared data (SSD) in a wireless communication system, a first party outputs a first random number as a first challenge wherein the first party is one of a network and a mobile. A second party generates a second random number in response to the first challenge. The second party is the mobile if the first party is the network, and the second party is the network if the first party is the mobile. The second party generates a first challenge response by performing a keyed cryptographic function (KCF) on the first challenge and the second random number using a secondary key, which is not the SSD and is derived from a root key. The second party then transfers the second random number, as a second challenge, and the first challenge response to the first party. The first party verifies the second party based on the first and second challenges and the first challenge response, generates a second challenge response by performing the KCF on the second challenge using the secondary key, and transfers the second challenge response to the second party. The second party verifies the first party based on the second challenge and the second challenge response. Both parties respectively establish the SSD based on the first and second challenges.

FIG. 4



EP 0 977 452 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 30 5705

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	BROWN D: "TECHNIQUES FOR PRIVACY AND AUTHENTICATION IN PERSONAL COMMUNICATIONSYSTEMS A WELL DESIGNED P&A TECHNIQUE IS NEVASSARY TO PROTECT ASSETS" , IEEE PERSONAL COMMUNICATIONS,US,IEEE COMMUNICATIONS SOCIETY, VOL. 2, NR. 4, PAGE(S) 6-10 XP000517584 ISSN: 1070-9916	1-4,7,8, 11-14, 19,20	H04D7/38 H04L9/08
Y	* the whole document *	9,10,21, 22	
Y	PARK CH -S: "ON CERTIFICATE-BASED SECURITY PROTOCOLS FOR WIRELESS MOBILE COMMUNICATION SYSTEMS" , IEEE NETWORK: THE MAGAZINE OF COMPUTER COMMUNICATIONS,IEEE INC. NEW YORK,US, VOL. 11, NR. 5, PAGE(S) 50-55 XP000699941 ISSN: 0890-8044 * page 51, line 54 - page 54, line 45 *	9,10,21, 22	
A	US 5 613 214 A (KAMACHI KENICHIRO ET AL) 18 March 1997 (1997-03-18) * page 6, line 50 - line 67 * * page 8, line 53 - line 67 * * page 9 - page 10 * * figures 2,3 *	1,2,4-6, 9-11, 14-22	TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04Q H04L
E	WO 99 38288 A (DSC TELECOM LP) 29 July 1999 (1999-07-29) * page 8, line 16 - page 24; figures 1,2A,28 *	1-4,7, 9-16, 19-22	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	18 October 2000	Psatha, H

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 99 30 5705

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on. The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

18-10-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5613214 A	18-03-1997	JP 2786092 B	13-08-1998
		JP 7115413 A	02-05-1995
		SE 9403507 A	19-04-1995
WO 9938288 A	29-07-1999	US 5991405 A	23-11-1999